CYBER GUIDANCE ISSUE 00257

GOOGLE CHROME UNDER ACTIVE ATTACKS

DATE ISSUED: 30th March 2022

IMPACT	LOW	MEDIUM	HIGH

EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

An urgent update has been issued by Google in relation to it's web browser application Google Chrome after confirming vulnerabilities were under active exploitation by attackers.

BREAKDOWN

Currently being tracked under CVE-2022-1096, there isn't much information publicly available regarding this "Type Confusion in v8" referring to the JavaScript engine used by the Google Chrome browser. The security update was released by Google on Friday after an anonymous researcher submitted the zero-day. The high-severity rating indicates why Google has released a patch that only contains a patch for a single vulnerability, leading to speculation that it must be a fairly dire case.

Microsoft Edge has also confirmed it is affected by the same vulnerability and urges users to update to the latest version as soon as possible.

REMEDIATION STEPS

- Urgently update to the latest version of Google Chrome 99.0.4844.84 for Windows, Mac, & Linux users
- Enable automatic updates on your Google Chrome Browser to enable patches to be pushed across and automatically installed.
- Update to the latest version of Microsoft Edge 99.0.1150.55

REFERENCES & RESOURCES

Google
https://support.google.com/chrome/answer/95414?hl=en&co=GENIE.Platform%3DDesktop
https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_25.html

Malware Bytes
https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/03/update-now-google-releases-emergency-patch-for-chrome-zero-day-used-in-the-wild/

Bleeping Computer
https://www.bleepingcomputer.com/news/security/emergency-google-chrome-update-fixes-zero-day-used-in-attacks/